PTO 02-2662

Japan, Kokai
2-205915

RECORD UNIT SECURITY CONTROL FORMAT
[Rekodo Tan'i Sekyuriti Seigyo Hoshiki]

Katsutoshi Muramatsu

UNITED STATES PATENT AND TRADEMARK OFFICE
Washington, D. C. May 2002

Translated by: Schreiber Translations, Inc.

Country	:	Japan
Document No.	:	2-205915
Document Type	:	Kokai
Language	:	Japanese
Inventors	:	Katsutoshi Muramatsu
Applicant	:	Fujitsu, Ltd.
IPC	:	G 06 F 3/06 12/14
Application Date	:	February 3, 1989
Publication Date	:	August 15, 1990
Foreign Language Title	:	Rekodo Tan'i Sekyuriti Seigyo Hoshiki
English Title	:	RECORD UNIT SECURITY CONTROL FORMAT

Specification /1

1. Title of the Invention:

RECORD UNIT SECURITY CONTROL FORMAT

2. Claim

A record unit security control format with the following characteristics: In a record unit security control format for protecting the security of records in the direct access memory device (18), into which record information becomes memorized based on a recording format which uses a count unit, a key unit, and a data unit,

The following are configured within the control device (14), which controls the aforementioned direct access memory device:

The control mechanism (16), which attaches security information which is used for the determination of (in)accessibility to record units, and

The security information inspection mechanism (17), which, in cases where records are decoded and encoded, determines the (in)accessibility by comparing for a potential match the designated security information and the security information attached to a record which serves as an access target.

---

[1]Numbers in the margin indicate pagination in the foreign text

3. Detailed explanation of the invention

(Summary)

It concerns a record unit security control format for protecting the security of records in a direct access memory device into which record information becomes memorized based on a recording format which uses a count unit, a key unit, and a data unit, whereas

Its objective to realize a security system which ensures a high degree of record unit security, whereas

It is constituted by configuring the following within a control device which controls a direct access memory device: A control mechanism which attaches security information which is used for the determination of (in)accessibility to record units and a security information inspection mechanism which, in cases where records are decoded and encoded, determines the (in)accessibility by comparing for a potential match the designated security information and the security information attached to a record which serves as an access target. /2

(Industrial application fields)

The present invention concerns a record unit security control format for protecting the security of records in a direct access memory device into which record information becomes memorized based on a recording format which uses a count unit, a key unit, and a data unit.

In response to advanceduses of computer systems, the technology for protecting the security of data wherein data can be encoded and decoded exclusively by truly authorized individuals has become increasingly more important. Depending on application fields, it may become necessary to define security protection units in terms of record units rather than large aggregates of data such as files.

(Prior art)

Various security formats such as access control, flow control, password input, etc. are conceivable in the context of preventing improper accesses to data handled by computer systems.

The security of data is realized by permitting the use of said data in relation exclusively to a properly authorized processing subject who uses said data. In a case where said data have been recorded on a direct access memory device (DASD) such as a magnetic disc device, etc., an I/O for said direct access memory device is issued, and it is necessary to execute protocols for referencing or modifying the memorized data under proper authority.

Volumes, files, etc. are conceivable as such security protection units, and the goal has mainly been realized in the prior art based on the control of an operating system (OS). No mechanism for assigning a security function to each record unit memorized in the direct access memory device has, however, been realized.

(Problems to be solved by the invention)

In a case where a single file is constituted by multiple records of variable lengths, it may become necessary to allow or prohibit the referencing and/or renewal of data in manners specific to the types of the individual records.

As far as the format of the prior art is concerned, however, the security function cannot be designated for the record unit, and accordingly, it has been necessary to classify files depending on security protection levels and to formulate a separate file by clustering a group of records with a mutually equivalent security protection level.

In such a case, it becomes unavoidable to access multiple files in the context of processing a series of data, which is problematic in that the routine becomes complicated, accompanied by increased burdens on the processing time and memory capacity.

The possibility of determining the (in)accessibility of data within a record which has been opened within a main memory device based on a software logic operation is also being contemplated, but it is impossible to directly prohibit an improper access of a record within a direct access memory device based solely on the software routine of a mainframe processing unit, which is problematic in that the security protection becomes insufficient.

In a case where security information is memorized and managed at a site different from that of a record which serves as a security protection target, furthermore, it is problematic in that an

additional security protection mechanism becomes necessary for preventing the tampering of the security information itself.

The objective of the present invention, which attempts to solve the aforementioned problems, is to realize a security system which affords a high degree of record unit security.

(Mechanism for solving the problems)

Figure 1 is a principle block for the present invention.

In Figure 1, (10) is a processing device which consists of a CPU, memory, etc., whereas (11) is an access request unit through which the access to each record is requested, whereas (12) is an input/output management unit which manages the input and/or output actions of the operating system, whereas (13) is a channel device, whereas (14) is a control device which controls devices connected with it, whereas (15) is a microprocessor (MPU), whereas (16) is a security information recording control mechanism, whereas (17) is a security information inspection mechanism, whereas (18) is a direct access memory device (e.g., disc pack device, etc.).

/3

The direct access memory device (18) is a device into which records which serve as security protection targets in the present invention are memorized, and it is constituted to memorize record information based on a recording format which uses the count unit (C), key unit (K), and the data unit (D). Incidentally, (HA) is a home address which shows the top of a track.

As far as the present invention is concerned, the security label (S) is designed to be attached to each record. The security label (S) is constituted by the level (L), which shows the hierarchical order of security, and the category (C), which shows the application range. Security labels (S) of the same contents are scheduled to be stored in the key unit (K) and data unit (D) in this example. The security label (S) is assigned to the key unit (K) and data unit (D) for purposes of enabling positioning vis-à-vis each record and the inspection of security during data encoding and/or decoding operations independently during or after the positioning operation and of elevating the processing speed.

For realizing the security by the record unit, the control device (14) possesses the security information recording control mechanism (16), which is based on farmware [sic], and the security information inspection mechanism (17).

The security information recording control mechanism (16) engages in a control protocol whereby records are encoded into the direct access memory device (18) via the count unit (C), key unit (K), and the data unit (D) while the security label (S) is being attached to said records.

The security information inspection mechanism (17) compares for a potential match the security information designated by a preceding channel command and the security label (S) attached to the record during the encoding and/or decoding of said record for the purpose of

controlling the determination of the (in)accessibility to said record.

(Functions)

As far as the present invention is concerned, the security information is attached to the records which are being stored in the direct access memory device (18) themselves, and the (in)accessibility to each record is checked by the control device (14) during a record encoding and/or decoding operation. The execution of an input/output request which ignores the security information therefore becomes prohibited by the control device (14), based on which the goal of the security protection of each record in the direct access memory device (18) can be achieved.

As far as the designation of the security information to be used for the determination of (in)accessibility is concerned, the security protection by the record unit can be realized by inducing the input/output management unit (12) to add a channel program for designating the security information before a user's channel program (CCW) without modifying the extant user's channel program.

The inspection of security is executed automatically by the control device (14), and therefore, there is virtually no software overhead imputed to the processing device (10).

(Application examples)

Figure 2 instantiates the record format of an application example of the present invention, whereas Figure 3 is a constitutional diagram for the disc control device of [said] application example of the present invention, whereas Figure 4 instantiates data encoding commands in [said] application example of the present invention, whereas Figure 5 instantiates the data encoding control of [said] application example of the present invention, whereas Figure 6 instantiates the security check of the data encoding operation of [said] application example of the present invention, whereas Figure 7 instantiates the data encoding commands of [said] application example of the present invention, whereas Figure 8 instantiates the data encoding control of [another] application example of the present invention, whereas Figure 9 instantiates the security check of the data encoding operation of [another] application example of the present invention.

The present invention handles the security protection of record information in a direct access memory device for recording records of variable lengths, namely the so-called "CKD-DASD." Its record format is shown in Figure 2. Its constitution is identical to that of the prior art except that information on the security label (S) is added.

The count unit (C) possesses the following sets of information:

* F: Flag (a display which indicates the pervasion of either the format of the prior art or an expanded format which possesses the security label (S) is additionally rendered as this flag);

* CC: Cylinder No.;

* HH: Head No.; /4

* R: Record No.;

* S: Length of the security label (newly configured);

* K: Length of the key unit;

* DD: Length of the data unit.

The security labels (S), furthermore, are recorded onto the respective tops of the key unit (K) and data unit (D). The contents of the security label (S) in the key unit (K) and the contents of the security label (S) in the data unit (D) are mutually identical.

Figure 3 (i) shows a constitutional example of the disc control device (20), which instantiates one application example of the present invention.

The disc control device (20), which is connected to a channel device of a higher hierarchical order and the disc pack device (24), which serves as a direct access memory device, controls said disc pack device (24). It possesses the channel interface (21) on the channel device side and the device interface (23) on the disc pack device (24) side. It additionally possesses the microprocessor (15), which controls their interface via a microprogram, and the data buffer (22).

The following are configured on the data buffer (22), as Figure 3 (ii) indicates: The security information save zone (25), the command buffer (26), in which channel commands are saved, the security information judgment result memory unit (27), in which judgment

results on security information are memorized, the count buffer (28), which pertains to inputted and/or outputted records, the key buffer (29), and the data buffer (30).

Figure 4 shows examples of channel commands which are used in cases where data on records to which the security label (S) has been attached are encoded. The channel program of this embodiment is formulated in terms of the commands (a) through (e) shown below:

(a): SSD: Security information designation command

This command is orchestrated for designating new security information. A label and a category corresponding to the security label (S) are designated by this SSD command. The level and the length may each be variably designated depending on applications.

(b): TIC: Branch command

The prevailing status is hereby branched into the channel program (CCW) formulated by the user. In other words, these commands (a) and (b) are each orchestrated for inducing the input/output management unit (12) shown in Figure 1 to add said commands to the channel program formulated by the access request unit (11).

(c): SID: Search ID command

(d): TIC: Branch command

(e): RD: Read data command

These commands (a) through (e) are equivalent to the commands which have been used in the prior art for accessing the CKD-DASD.

In response to the channel commands shown in Figure 4, the

microprocessor (15) of the disc control device (20) shown in Figure 3 engages in the control routine shown in Figure 5:

(a): In response to the SSD command, the security information designated by the command is saved into the security information save zone (25) of the data buffer (22);

(b): Next, in response to the TIC command, the prevailing status is branched into the following user CCW for enabling data encoding;

(c): In response to the SID command, the count unit of the record is encoded into the data buffer (22) from the direct access memory device, and whether or not it is the count unit of the designated record is inspected. In a case where a non-designated position has been judged, the count unit inspection is repeated until the completion of the search;

In a case where it has been judged to be the count unit of the designated position, the security label (S) of the key unit or data unit and the security information saved into the security information save zone (25) are compared for a potential match, and the (in)feasibility of positioning is thus determined;

(d): In a case where the positioning is "feasible," a transition is made to the stage next to the TIC command, whereas in a case where the same is "infeasible," the search of (c) is repeated;

(e): In response to the RD command, the security information of the data unit is compared, and in an accessible case, the data of the data unit are encoded, whereas in an inaccessible case, an I/O error is judged. This check of the security information may be dispensed

with in a case where this RD command is chained to the SID + TIC commands. The check is indispensable in a case where it is chained to the commands of a READ system or WRITE system.

/5

A case where the security information shown in Figure 6 (i) has been designated by the SSD command during the encoding of data may, for example, be hypothesized. A higher value of the level information L signifies a higher security order. The category information C is defined by a 1-bit flag depending on the type of information. The level and category designated by the SSD command are hereby assumed to be SSD-L and SSD-C, respectively, and the level and category of the security label (S) which is being designated within the record as record-L and record-C, respectively, and in such a case, the conditions for enabling the encoding of data are stipulated as follows:

$$\text{SSD-L} \geq \text{record-L AND}$$

$$\text{SSD-C} \supset \text{record-C.}$$

In a case where data are encoded into the records shown in Figure 6 (ii) based on the designation of the security information shown in Figure 6 (i), the encodings of the first and second records become possible under the aforementioned security conditions. In a case where encoding into the third record becomes commanded, an I/O error is judged due to a level mismatch.

Figures 6 (iii) and (iv) show another example.

In a case where data are encoded into the records shown in Figure 6 (iv) based on the designation of the security information shown in Figure 6 (iii), the encoding of the first record is impossible due to a failure to meet the category requirement, and the encoding of the third record is impossible due to a level mismatch. Thus, only the second record is encodable.

Figure 7 shows examples of channel commands which are used in a case where data are encoded into records to which the security label (S) has been attached. The commands of (a) through (d) are comparable to the data encoding commands shown in Figure 4, whereas the WD command of (e) is a command which instructs the encoding of data.

In response to these channel commands shown in Figure 7, the microprocessor (15) of the disc control device (20) shown in Figure 3 engages in the control routine shown in Figure 8.

(a): In response to the SSD command, the security information designated by said command is saved into the security information save zone (25) of the data buffer (22).

(b): Next, in response to the TIC command, the prevailing status is branched into the following user CCW for enabling data encoding;

(c): In response to the SID command, the count unit of the record is encoded into the data buffer (22) from the direct access memory device, and whether or not it is the count unit of the designated record is inspected. In a case where a non-designated position has been judged, the count unit inspection is repeated until the completion of the search;

In a case where it has been judged to be the count unit of the designated position, the security label (S) of the key unit or data unit and the security information saved into the security information save zone (25) are compared for a potential match, and the (in)feasibility of positioning is thus determined;

(d): In a case where the positioning is "feasible," a transition is made to the stage next to the TIC command, whereas in a case where the same is "infeasible," the search of (c) is repeated;

(e): In response to the WD command, the security information of the data unit is compared, and in an accessible case, the data of the data unit are encoded, whereas in an inaccessible case, an I/O error is judged. This check of the security information may be dispensed with in a case where this RD command is chained to the SID + TIC commands. The check is indispensable in a case where it is chained to the commands of a READ system or WRITE system.

A case where the security information shown in Figure 9 (i) has been designated by the SSD command during the encoding of data may, for example, be hypothesized. The level and category designated by the SSD command are hereby assumed to be SSD-L and SSD-C, respectively, and the level and category of the security label (S) which is being designated within the record as record-L and record-C, respectively, and in such a case, the conditions for enabling the encoding of data are stipulated as follows (opposite of that under the conditions of the READ mode):

$$\text{SSD-L} \leq \text{record-L AND}$$

SSD-C ⊂ record-C. /6

In a case where data are encoded into the records shown in Figure 9 (ii) based on the designation of the security information shown in Figure 9 (i), the encodings of the second and third records become possible under the aforementioned security conditions. In a case where encoding into the first record becomes commanded, an I/O error is judged due to a level mismatch.

Figures 9 (iii) and (iv) show another example.

In a case where data are encoded into the records shown in Figure 9 (iv) based on the designation of the security information shown in Figure 9 (iii), the only encodable record is the third record by default.

Incidentally, in the context of handling the security information, various commands other than the SSD command may, if necessary, be easily supported by redesignating the farmware in the control device. In order to achieve interchangeability, for example, in the cases of a command for synchronously encoding the count unit, key unit, and the data unit (READ CKD command), notifications are rendered after the information of the security label (S) has been removed. The following commands, furthermore, are designated anew for decoding the security label (S): (1): READ C & S command; (2): READ K & S command' (3): READ KD & S command; (4): READ CKD & S command; etc. Commands specific to the format for designating the security label (S) are likewise prepared for commands for the WRITE system.

(Effects of the invention)

As the foregoing explanations have demonstrated, the present invention enables none other than authorized subjects to encode and decode based on the attachment of security information to records, based on which a security system with a high level of security can be realized while the security protection range is being defined in terms of the record unit. Since the records themselves possess the security information, furthermore, the loss of protection in response to transfers of data can be avoided, and improper uses (e.g., copy, etc.) can also be prevented.

4. Brief explanation of the figures

Figure 1 is a principle block for the present invention.

Figure 2 instantiates the record format of an application example of the present invention.

Figure 3 is a constitutional diagram for the disc control device of [said] application example of the present invention.

Figure 4 instantiates data encoding commands in [said] application example of the present invention.

Figure 5 instantiates the data encoding control of [said] application example of the present invention.

Figure 6 instantiates the security check of the data encoding operation of [said] application example of the present invention.

Figure 7 instantiates the data encoding commands of [said] application example of the present invention.

Figure 8 instantiates the data encoding control of [another] application example of the present invention.

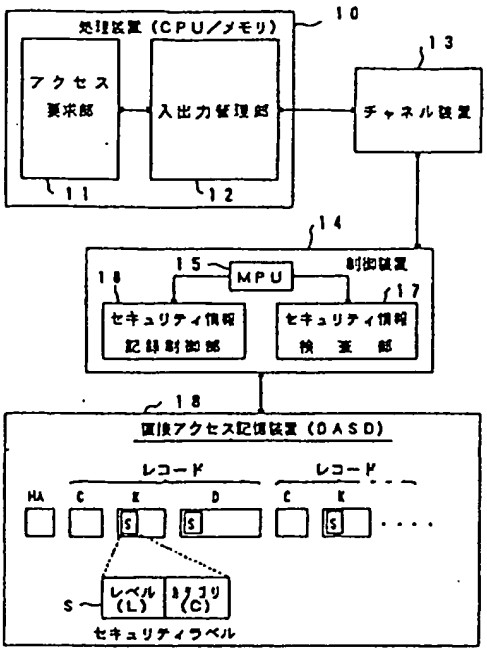
Figure 9 instantiates the security check of the data encoding operation of [another] application example of the present invention.

In the figures, the notations denote the following: (10): Processing device; (11): Access request unit; (12): Input/output management unit; (13): Channel device; (14): Control device; (15): Microprocessor; (16): Security information recording control mechanism; (17): Security information inspection mechanism; (18): Direct access memory device; (S): Security label.

Patent Applicant: Fujitsu, Ltd.

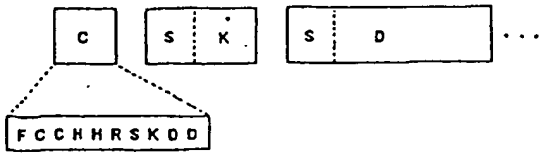
Agents: Kichiyoshi Ogasawara, patent attorney (and two others)

Figure 1



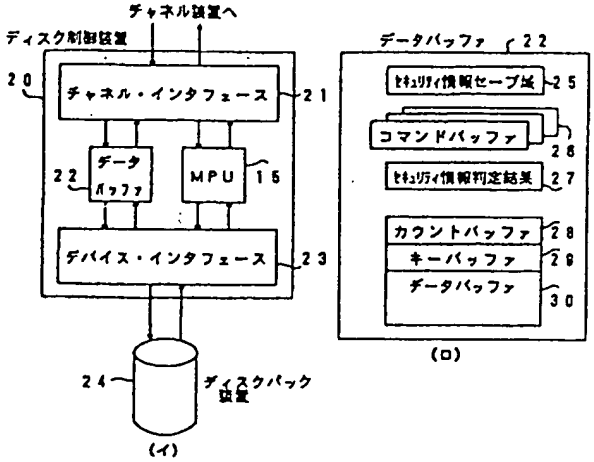
[(0): Principle block diagram of the present invention; (10): Processing device (CPU/memory); (11): Access request unit; (12): Input/output management unit; (13): Channel device; (14): Control device; (16): Security information recording control mechanism; (17): Security information inspection mechanism; (18): Direct access memory device (D & SD); (R): Record; (S): Security label; (L): Label; (C): Category]

Figure 2



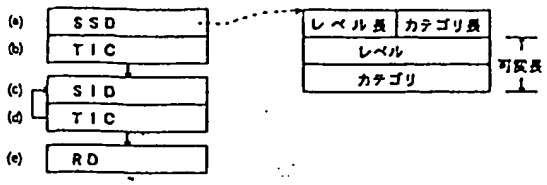
[(0): Example of record format]

Figure 3



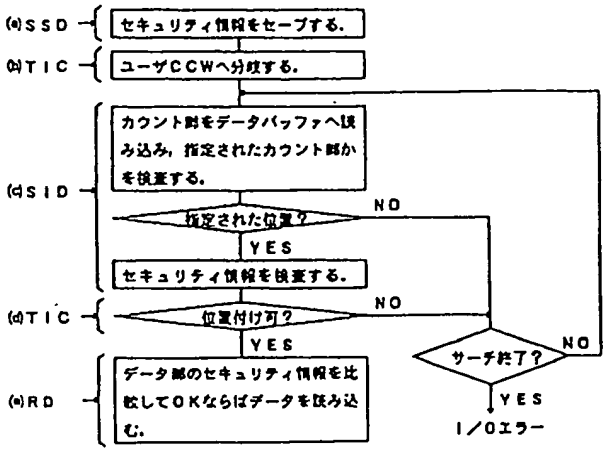
[(0): Disc control device constitutional diagram; (C): To channel device; (20): Disc control device; (21): Channel interface; (22): Data buffer; (23): Device interface; (24): Disc pack device; (25): Security information save zone; (26): Command buffer; (27): Security information judgment result memory unit; (28): Count buffer; (29): Key buffer; (30): Data buffer]

Figure 4



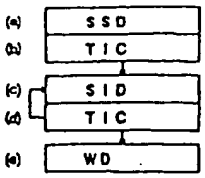
[(0): Examples of data encoding commands; (1): Level length; (2): Category length; (3): Level; (4): Category; (5): Variable length]

Figure 5



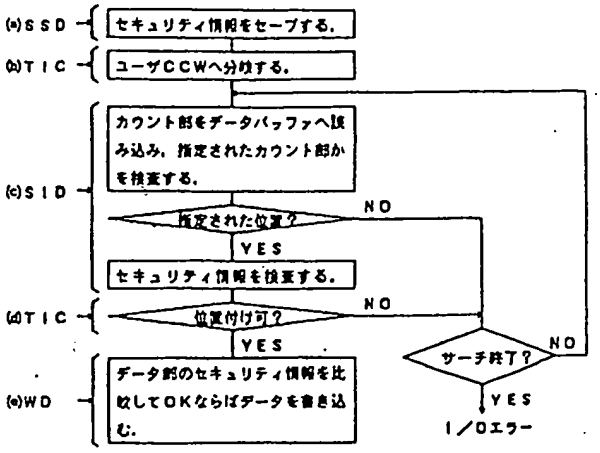
[(0): Example of data encoding control; (1): Saving of security information; (2): Branching into user CCW; (3): Encoding of count unit into data buffer and inspection of its coincidence with designated count unit or lack thereof; (4): Designated position?; (5): Inspection of security information; (6): Positioning feasible?; (7): Comparison of security information of data unit and encoding of data if OK; (8): Search complete?; (8): I/O error]

Figure 7



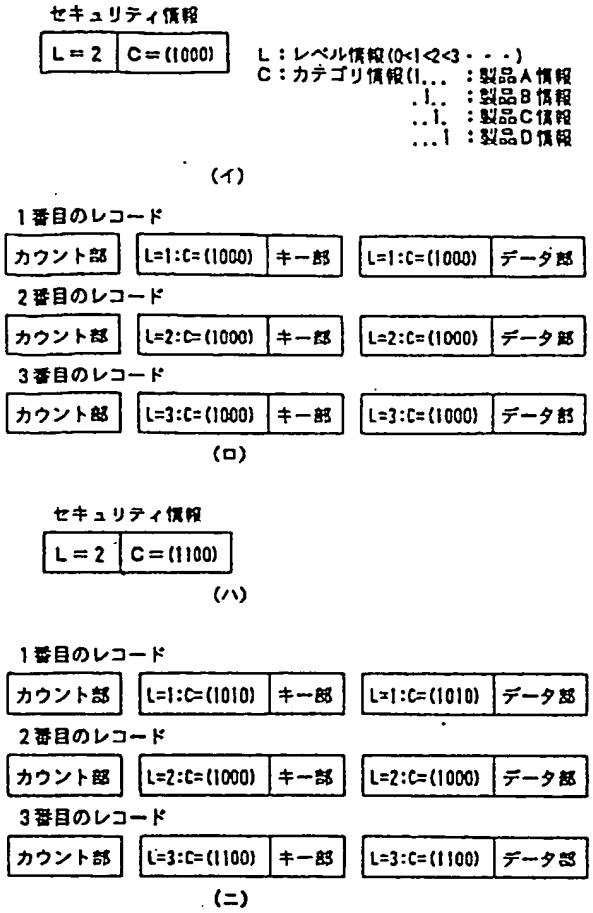
[(0): Examples of data encoding commands]

Figure 8



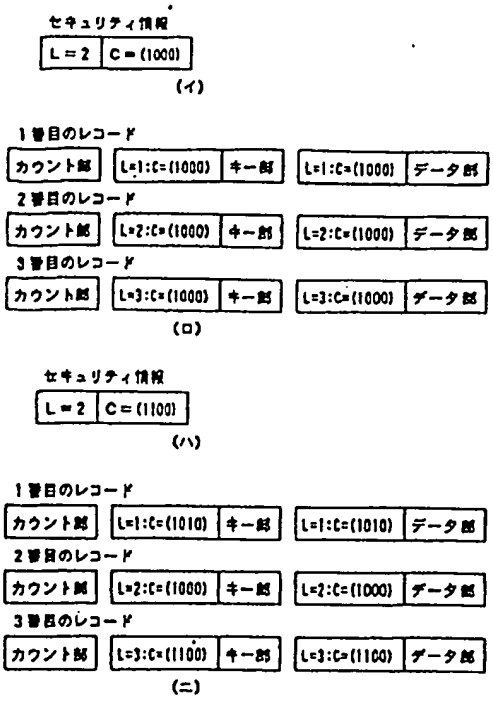
[(0): Example of data encoding control; (1): Saving of security information; (2): Branching into user CCW; (3): Encoding of count unit into data buffer and inspection of its coincidence with designated count unit or lack thereof; (4): Designated position?; (5): Inspection of security information; (6): Positioning feasible?; (7): Comparison of security information of data unit and encoding of data if OK; (8): Search complete?; (8): I/O error]

Figure 6 /8



[(0): Example of security check during data encoding; (1): First record; (2): Second record; (3): Third record; (4): Product A information; (5): Product B information; (6): Product C information; (7): Product D information; (L): Level information; (C'): Category information; (C): Count unit; (K): Key unit; (D): Data unit; (S): Security label]

Figure 9



[(0): Example of security check during data encoding; (1): First record; (2): Second record; (3): Third record; (C): Count unit; (K): Key unit; (D): Data unit; (S): Security label]

⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平2-205915

⑤1Int.Cl.⁵	識別記号	庁内整理番号	⑬公開　平成2年(1990)8月15日
G 06 F 3/06	304 H	6711-5B	
12/14	320 A	7737-5B	

審査請求　未請求　請求項の数 1　(全8頁)

⑤4発明の名称　レコード単位セキュリテイ制御方式

⑳特　願　平1-25219
㉒出　願　平1(1989)2月3日

㉗発明者　村松　勝利　神奈川県川崎市中原区上小田中1015番地　富士通株式会社内
㉑出願人　富士通株式会社　神奈川県川崎市中原区上小田中1015番地
㉔代理人　弁理士　小笠原　吉義　外2名

明　細　書

1．発明の名称

レコード単位セキュリティ制御方式

2．特許請求の範囲

カウント部，キー部，データ部を有する記録フォーマットによって，レコード情報の記憶が行われる直接アクセス記憶装置(18)におけるレコードの機密保護を行うレコード単位セキュリティ制御方式であって，

上記直接アクセス記憶装置をコントロールする制御装置(14)内に，

レコード単位にアクセス可否の決定に使用されるセキュリティ情報を付加して直接アクセス記憶装置内に記録する制御手段(16)と，

レコードの読み出しおよび書き込み時に，指定されたセキュリティ情報と，アクセス対象となるレコードに付加されたセキュリティ情報との照合により，アクセス可否を決定するセキュリティ情報検査手段(17)とを備えたことを特徴とするレコード単位セキュリティ制御方式。

3．発明の詳細な説明

(概要)

カウント部，キー部，データ部を有する記録フォーマットによって，レコード情報の記憶が行われる直接アクセス記憶装置におけるレコードの機密保護を行うレコード単位セキュリティ制御方式に関し，

レコード単位の高密度のセキュリティシステムを実現可能とすることを目的とし，

直接アクセス記憶装置をコントロールする制御装置内に，レコード単位にアクセス可否の決定に使用されるセキュリティ情報を付加して直接アクセス記憶装置内に記録する制御手段と，レコードの読み出しおよび書き込み時に，指定されたセキュリティ情報と，アクセス対象となるレコードに付加されたセキュリティ情報との照合により，アクセス可否を決定するセキュリティ情報検査手段

とを備えるように構成する。

〔産業上の利用分野〕

本発明は，カウント部，キー部，データ部を有する記録フォーマットによって，レコード情報の記憶が行われる直接アクセス記憶装置におけるレコードの機密保護を行うレコード単位セキュリティ制御方式に関する。

計算機システムの高度な利用により，真に権限を持つ者だけがデータを読み書きできるようなデータの機密保護の技術がますます重要になってきている。応用分野によっては，機密保護の単位を，ファイルのようなデータの大きな集合だけではなく，レコード単位とすることが必要になる場合がある。

〔従来の技術〕

計算機システムが扱うデータに対して，不当なアクセスを防ぐために，アクセス制御，フロー制御，暗号化など，種々のセキュリティ方式が考えられている。

データのセキュリティは，データを使用する正当な権限のある処理主体にのみ，そのデータの使用を許可することにより実現される。データが，磁気ディスク装置などの直接アクセス記憶装置（ＤＡＳＤ）に記録されたものである場合には，その直接アクセス記憶装置に対するＩ／Ｏを発行し，それに記憶されたデータを参照したり，変更したりすることが，正しい権限のもとで行われる必要がある。

このような機密保護の単位としては，ボリュームやファイルなどがあり，従来，主としてオペレーティング・システム（ＯＳ）の制御によって実現されている。しかしながら，直接アクセス記憶装置に記録されている各レコード単位に，セキュリティ機能を設定する手段は実現されていなかった。

〔発明が解決しようとする課題〕

１つのファイルが，多数の可変長レコードから構成される場合に，個々のレコードの種類ごとに，そのデータに対する参照または更新を許可したり，禁止したりすることができるようにすることが必要になる場合がある。

しかし，従来方式では，レコード単位にセキュリティ機能を設定することができないため，機密保護レベルに応じてファイルを分割し，それぞれ機密保護レベルが同等なレコード群をまとめて，別々なファイルとして作成する必要があった。

この場合，一連のデータ処理において，多数のファイルをアクセスしなければならないようなことが起こり，処理が複雑化するとともに，処理時間やメモリが多く必要になるという問題があった。

また，ソフトウェアによる論理操作によって，主記憶装置に展開されたレコード内のデータの使用可否を決定することも考えられているが，本体系処理装置のソフトウェアによる対処だけでは，直接アクセス記憶装置におけるレコードの不当なアクセスを，直接禁止することができないので，機密保護が十分ではないという問題があった。

また，セキュリティ情報を，その機密保護対象となるレコードとは別の場所で記憶し管理する場合には，セキュリティ情報自体の改ざん防止のために，さらにその機密保護手段が必要になるという問題があった。

本発明は上記問題点の解決を図り，レコード単位の高密度のセキュリティシステムを実現可能とすることを目的としている。

〔課題を解決するための手段〕

第１図は本発明の原理ブロック図を示す。

第１図において，１０はＣＰＵおよびメモリなどからなる処理装置，１１は各レコードに対するアクセス要求を行うアクセス要求部，１２はオペレーティング・システムにおける入出力動作を管理する入出力管理部，１３はチャネル装置，１４は配下に接続される装置をコントロールする制御装置，１５はマイクロプロセッサ（ＭＰＵ），１６はセキュリティ情報記録制御部，１７はセキュリティ情報検査部，１８はディスクパック装置な

どの直接アクセス記憶装置を表す。

直接アクセス記憶装置１８は，本発明において秘密保護の対象とするレコードを記憶する装置であって，カウント部Ｃ，キー部Ｋ，データ部Ｄを有する記録フォーマットにより，レコード情報を記憶するようになっている。なお，ＨＡはトラックの先頭を示すホームアドレスである。

本発明では，各レコードにセキュリティラベルＳが付加されるようになっている。セキュリティラベルＳは，秘密度の程度を示すレベル（Ｌ）と，適用範囲を示すカテゴリ（Ｃ）とからなる。この例では，セキュリティラベルＳは，キー部Ｋとデータ部Ｄとに，同内容のものが格納されるようになっている。キー部Ｋとデータ部Ｄとに，セキュリティラベルＳを持つのは，レコードへの位置付けやデータの読み書きにおけるセキュリティの検査を，位置付け時または位置付け後にそれぞれ独立に行うことができるようにし，処理を高速化するためである。

このセキュリティラベルＳにより，レコード単位のセキュリティを実現するために，制御装置１４は，ファームウェアによるセキュリティ情報記録制御部１６と，セキュリティ情報検査部１７とを持つ。

セキュリティ情報記録制御部１６は，レコードのカウント部Ｃ，キー部Ｋ，データ部Ｄを，直接アクセス記憶装置１８に書き込むときに，セキュリティラベルＳを付与して記録する制御を行う。

セキュリティ情報検査部１７は，レコードの読み出しおよび書き込み時に，先行するチャネルコマンドによって指定されたセキュリティ情報と，レコードに付加されたセキュリティラベルＳとの照合により，そのレコードに対するアクセス可否を決定する制御を行うようになっている。

〔作用〕

本発明では，直接アクセス記憶装置１８に格納されたレコード自体に，セキュリティ情報が付加され，レコードの読み出しおよび書き込み時には，制御装置１４によって，各レコードに対するアクセス可否のチェックが行われる。したがって，セキュリティ情報を無視した入出力要求は，制御装置１４により，その実行が抑止され，直接アクセス記憶装置１８における各レコードの秘密保護が達成される。

アクセス可否の決定に使用するセキュリティ情報の指定は，ユーザのチャネルプログラム（ＣＣＷ）の前に，入出力管理部１２が，セキュリティ情報を設定するチャネルプログラムを付加するようにすれば，現状のユーザのチャネルプログラムを変更することなく，レコード単位の秘密保護を図ることができる。

セキュリティの検査は，制御装置１４によって自動的に行われるので，処理装置１０におけるソフトウェアのオーバヘッドはほとんどない。

〔実施例〕

第２図は本発明の実施例によるレコード形式の例，第３図は本発明の実施例に係るディスク制御装置構成図，第４図は本発明の実施例によるデータ読み込みコマンドの例，第５図は本発明の実施例によるデータ読み込み制御の例，第６図は本発明の実施例によるデータ読み込み時のセキュリティ・チェックの例，第７図は本発明の実施例によるデータ書き込みコマンドの例，第８図は本発明の実施例によるデータ書き込み制御の例，第９図は本発明の実施例によるデータ書き込み時のセキュリティ・チェックの例を示す。

本発明は，可変長レコードを記録する直接アクセス記憶装置，いわゆるＣＫＤ－ＤＡＳＤにおけるレコード情報の秘密保護を扱う。そのレコード形式は，第２図に示すようになっている。セキュリティラベルＳに関する情報が付加されること以外は，従来と同様な構成である。

カウント部Ｃは，次の情報を持つ。

・Ｆ：フラグ（このフラグとして，従来形式であるか，セキュリティラベルＳを持つ拡張形式であるかの表示が追加される）。
・ＣＣ：シリンダ番号。
・ＨＨ：ヘッド番号。

・Ｒ：レコード番号。
・Ｓ：セキュリティラベルの長さ（新設）。
・Ｋ：キー部の長さ。
・ＤＤ：データ部の長さ。

また，キー部Ｋとデータ部Ｄの先頭に，それぞれセキュリティラベルＳが記録される。キー部Ｋにおけるセキュリティラベルの内容と，データ部Ｄにおけるセキュリティラベルの内容とは同じである。

第３図（イ）は，本発明の実施例であるディスク制御装置２０の構成例を示している。

ディスク制御装置２０は，上位のチャネル装置と，直接アクセス記憶装置であるディスクパック装置２４との間に接続され，ディスクパック装置２４をコントロールする。チャネル装置側にチャネル・インタフェース２１を有し，ディスクパック装置２４側にデバイス・インタフェース２３を有する。また，これらのインタフェースをマイクロプログラムによって制御するマイクロプロセッサ１５と，データバッファ２２とを持つ。

データバッファ２２には，第３図（ロ）に示すように，セキュリティ情報セーブ域２５，チャネルコマンドが格納されるコマンドバッファ２６，セキュリティ情報の判定結果を記憶するセキュリティ情報判定結果記憶部２７および入出力レコードに関するカウントバッファ２８，キーバッファ２９，データバッファ３０が設けられる。

第４図は，セキュリティラベルＳが付加されたレコードのデータを読み込む場合に使用するチャネルコマンドの例を示している。ここでは，以下のような(a)～(e)のコマンドによってチャネルプログラムが作成されている。

(a)　ＳＳＤ：セキュリティ情報設定コマンド

新しくセキュリティ情報を指定するために設けられたコマンドである。このＳＳＤコマンドでは，セキュリティラベルＳに対応するレベルとカテゴリとを指定する。レベルおよびカテゴリの長さは，それぞれ用途に応じて変化し，可変長である。

(b)　ＴＩＣ：分岐コマンド

ここから，ユーザが作成したチャネルプログラム（ＣＣＷ）に分岐する。すなわち，この(a)，(b)のコマンドは，第１図に示す入出力管理部１２が，アクセス要求部１１が作成したチャネルプログラムに付加するようにしたコマンドである。

(c)　ＳＩＤ：サーチＩＤコマンド
(d)　ＴＩＣ：分岐コマンド
(e)　ＲＤ：リードデータコマンド

この(c)～(e)のコマンドは，ＣＫＤ－ＤＡＳＤに対するアクセスに，従来から使用されているコマンドである。

第４図に示すようなチャネルコマンドに対し，第３図に示すディスク制御装置２０のマイクロプロセッサ１５は，第５図に示すような制御を行う。

(a)　ＳＳＤコマンドに対して，データバッファ２２におけるセキュリティ情報セーブ域２５に，コマンドで指定されたセキュリティ情報を退避する。

(b)　次にＴＩＣコマンドに対して，データ読み込みを行う以下のユーザＣＣＷへ分岐する。

(c)　ＳＩＤコマンドに対して，直接アクセス記憶装置から，レコードのカウント部をデータバッファ２２へ読み込み，指定されたレコードのカウント部かどうかを検査する。指定された位置ではない場合，サーチが終了するまで，カウント部の検査を繰り返す。

指定された位置のカウント部である場合，次にキー部またはデータ部のセキュリティラベルＳと，セキュリティ情報セーブ域２５に退避したセキュリティ情報とを比較照合し，位置付けの可否を決定する。

(d)　位置付けが「可」である場合，ＴＩＣコマンドの次に移る。「不可」であれば，(c)のサーチを繰り返す。

(e)　ＲＤコマンドに対し，データ部のセキュリティ情報を比較して，アクセス可であれば，データ部のデータを読み込む。アクセス不可の場合，Ｉ／Ｏエラーとする。ここでのセキュリティ情報のチェックは，このＲＤコマンドが，ＳＩＤ＋ＴＩＣのコマンドにチェインされていた場合には，省略することができる。ＲＥＡＤ系またはＷＲＩＴＥ系のコマンドにチェインされていた場合には，

必ずチェックを行う。

例えば，データの読み込み時に，第6図（イ）に示すセキュリティ情報を，ＳＳＤコマンドで指定したとする。レベル情報Ｌは，値が大きいほうが機密度が高い。カテゴリ情報Ｃは，ここでは情報の種類ごとに，１ビットのフラグで定義している。今，ＳＳＤコマンドで指定したレベルおよびカテゴリを，ＳＳＤ－Ｌ，ＳＳＤ－Ｃとし，レコード内に設定されているセキュリティラベルＳのレベルおよびカテゴリを，レコード－Ｌ，レコード－Ｃとすると，データ読み込みが可能である条件は，以下のとおりである。

ＳＳＤ－Ｌ≦レコード－Ｌ　かつ

ＳＳＤ－Ｃ⊃レコード－Ｃ

第6図（イ）に示すセキュリティ情報の指定により，第6図（ロ）に示すようなレコードに対するデータの読み込みが行われた場合，上記セキュリティ条件により，１番目と２番目のレコードは，読み込み可となる。３番目のレコードに対して，読み込みが指示されたとすると，レベルが合わないため，Ｉ／Ｏエラーとなる。

第6図（ハ），（ニ）は，他の例を示している。

第6図（ハ）に示すセキュリティ情報の指定により，第6図（ニ）に示すようなレコードに対するデータの読み込みが行われた場合，１番目のレコードは，カテゴリが満足しないので，読み込み不可である。３番目のレコードは，レベルが合わないので，読み込み不可である。したがって，２２番目だけが読み込み可能なレコードとなる。

第7図は，セキュリティラベルＳが付加されたレコードに，データを書き込む場合に使用するチャネルコマンドの例を示している。(a)～(d)のコマンドは，第4図に示したデータ読み込み時におけるコマンドと同様であり，(e)のＷＤコマンドは，データを書き込むことを指示するコマンドである。

この第7図に示すチャネルコマンドに対し，第3図に示すディスク制御装置２０のマイクロプロセッサ１５は，第8図に示すような制御を行う。

(a)　ＳＳＤコマンドに対して，データバッファ２２におけるセキュリティ情報セーブ域２５に，コマンドで指定されたセキュリティ情報を退避する。

(b)　次にＴＩＣコマンドに対して，データ読み込みを行う以下のユーザＣＣＷへ分岐する。

(c)　ＳＩＤコマンドに対して，直接アクセス記憶装置から，レコードのカウント部をデータバッファ２２へ読み込み，指定されたレコードのカウント部かどうかを検査する。指定された位置ではない場合，サーチが終了するまで，カウント部の検査を繰り返す。

指定された位置のカウント部である場合，次にキー部またはデータ部のセキュリティラベルＳと，セキュリティ情報セーブ域２５に退避したセキュリティ情報とを比較照合し，位置付けの可否を決定する。

(d)　位置付けが「可」である場合，ＴＩＣコマンドの次に移る。「不可」であれば，(c)のサーチを繰り返す。

(e)　ＷＤコマンドに対し，データ部のセキュリティ情報を比較して，アクセス可であれば，データ部のデータを書き込む。アクセス不可の場合，Ｉ／Ｏエラーとする。ここでのセキュリティ情報のチェックは，このＷＤコマンドが，ＳＩＤ＋ＴＩＣのコマンドにチェインされていた場合には，省略することができる。ＲＥＡＤ系またはＷＲＩＴＥ系のコマンドにチェインされていた場合には，必ずチェックを行う。

例えば，データの書き込み時に，第9図（イ）に示すセキュリティ情報を，ＳＳＤコマンドで指定したとする。ＳＳＤコマンドで指定したレベルおよびカテゴリを，ＳＳＤ－Ｌ，ＳＳＤ－Ｃとし，レコード内に設定されているセキュリティラベルＳのレベルおよびカテゴリを，レコード－Ｌ，レコード－Ｃとすると，データ書き込みが可能である条件は，以下のとおりである（ＲＥＡＤ時の条件とは逆の関係になる）。

ＳＳＤ－Ｌ≦レコード－Ｌ　かつ

ＳＳＤ－Ｃ⊂レコード－Ｃ

第9図（イ）に示すセキュリティ情報の指定により，第9図（ロ）に示すようなレコードに対するデータの書き込みが行われた場合，上記セキュ

リティ条件により，2番目と3番目のレコードは，書き込み可となる．1番目のレコードに対して，書き込みが指示されたとすると，レベルが合わないため，I／Oエラーとなる．

第9図（ハ），（ニ）は，他の例を示している．

第9図（ハ）に示すセキュリティ情報の指定により，第9図（ニ）に示すようなレコードに対するデータの書き込みが行われた場合，結果として書き込み可能なレコードは，3番目のレコードだけとなる．

なお，セキュリティ情報の扱いについて，SSDコマンド以外に，必要に応じて種々のコマンドをサポートすることは，制御装置におけるファームウェアの変更により，容易に対処することができる．例えば，互換性のため，カウント部，キー部，データ部を合わせて読み込むコマンド（READ CKDコマンド）では，セキュリティラベルSの情報を取り除いて通知する．セキュリティラベルSを読むために，次のようなコマンド．

① READ C&Sコマンド
② READ K&Sコマンド
③ READ KD&Sコマンド
④ READ CKD&Sコマンド

などを新設する．WRITE系のコマンドに対しても，同様にセキュリティラベルSを設定するフォーマット用のコマンドを用意する．

〔発明の効果〕

以上説明したように，本発明によれば，レコードにセキュリティ情報を付加することにより，権限を持つ処理主体だけが，読み書きできるようになるので，セキュリティ保護範囲をレコード単位として，高密度のセキュリティシステムを実現することができるようになる．また，セキュリティ情報をレコードに持つので，データの移動に対しても保護が外れることがなくなり，コピーなどの不正使用についても防止することができる．

4．図面の簡単な説明

第1図は本発明の原理ブロック図．

第2図は本発明の実施例によるレコード形式の例．

第3図は本発明の実施例に係るディスク制御装置構成図．

第4図は本発明の実施例によるデータ読み込みコマンドの例．

第5図は本発明の実施例によるデータ読み込み制御の例．

第6図は本発明の実施例によるデータ読み込み時のセキュリティ・チェックの例．

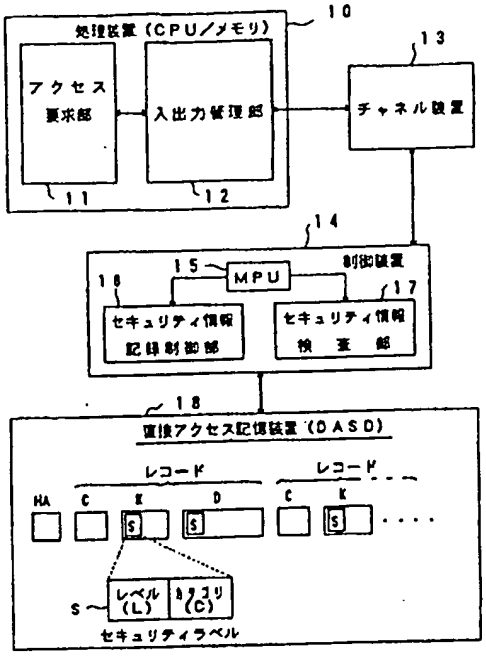
第7図は本発明の実施例によるデータ書き込みコマンドの例．

第8図は本発明の実施例によるデータ書き込み制御の例．

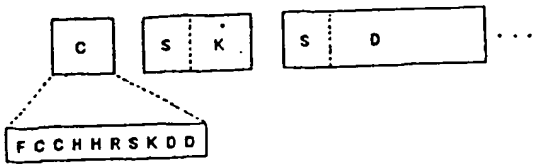
第9図は本発明の実施例によるデータ書き込み時のセキュリティ・チェックの例を示す．

図中，10は処理装置，11はアクセス要求部，12は入出力管理部，13はチャネル装置，14は制御装置，15はマイクロプロセッサ，16はセキュリティ情報記録制御部，17はセキュリティ情報検査部，18は直接アクセス記憶装置，Sはセキュリティラベルを表す．

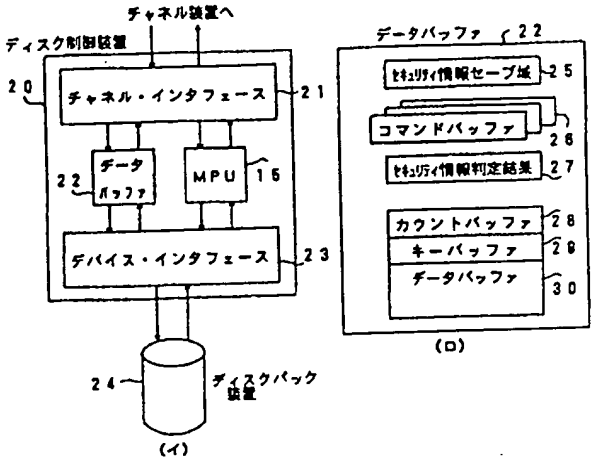
特許出願人　富士通株式会社
代理人　弁理士　小笠原吉義（外2名）



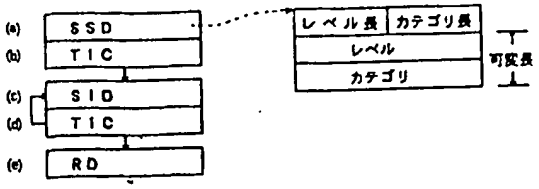
本発明の原理ブロック図
第 1 図



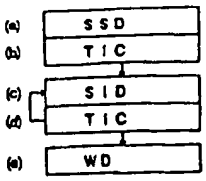
レコード形式の例
第 2 図



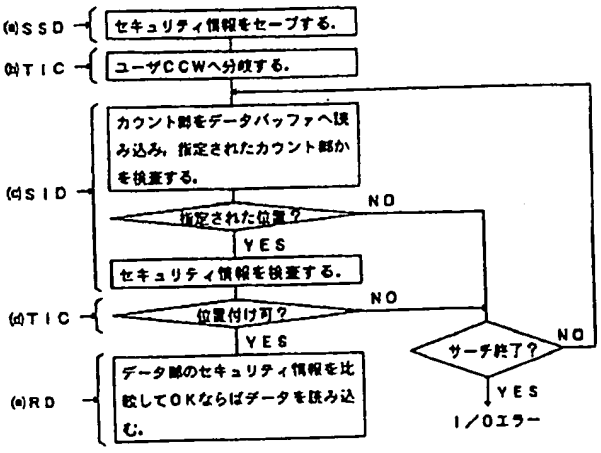
ディスク制御装置構成図
第 3 図



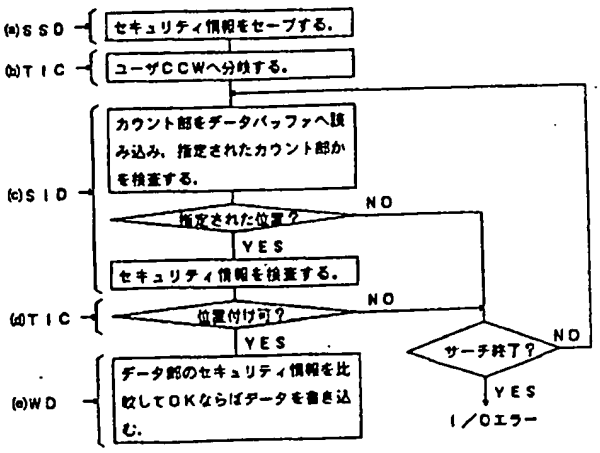
データ読み込みコマンドの例
第 4 図



データ書き込みコマンドの例
第 7 図



データ読み込み制御の例
第 5 図



データ書き込み制御の例
第 8 図

データ読み込み時のセキュリティ・チェックの例

第 6 図

データ書き込み時のセキュリティ・チェックの例

第 9 図